Post Exercise Overview

SILENT VECTOR

Andrews Air Force Base
October 17-18, 2002

**Purpose of the exercise:**

To explore the difficulties of coping with credible warning of a terrorist attack, but with insufficient information for effective prevention

**Organization:**

A simulated emergency meeting of the National Security Council at Camp David. All participants were former government officials with relevant experience

**Scenario:**

Imprecise but credible warning of attack against energy and energy related infrastructure on the East Coast to include:

- Nuclear Power Plants
- Refineries
- Large LNG/LPG Storage Operations
- Pipeline Infrastructure
- Petroleum Terminals
- Chemical Operations
- Dams

Role players had no knowledge of types of targets or modes of attack at the beginning of the exercise. Intelligence indicated that the attack would occur in two days, but timing remained questionable. In addition, intelligence indicated that multiple attack teams were likely and probably already in place somewhere in the United States.
**Threat/Vulnerability Analysis/Integration:**

A “Threat Vulnerability Analysis/Integration” methodology was developed to support the exercise. It was presented to the NSC as the product of 36 hours of staff analysis.

**Key Developments:** Leaders considered initial threat information too vague for concrete plans:

Leaders ordered sensible protection steps and set a future date for a press conference.

Word leaks out as a result of the sensible protective measures taken.

Communities would seem pre-disposed to panic (those with nuclear power plants, for example) assume the worst case scenario.

Leaders debate how to balance managing the panic versus managing the prevention of the attack.

Subsequent scenario developments confirm the risk and firm up the time of attack.

Leaders ground general aviation and cargo air traffic, plea for calm in citizenry.

Evacuations ordered in one location because of likely threat.

Luck (accident, fortuitous arrest of one terrorist) and grounding of general aviation blunt attack.

Not known at the time, however leaders confront quiet the day after expected attack date.

Was the attack foiled, deterred, or was it a hoax?

**Key Lesson #1:** When Governments can’t say what is happening, rumors become facts:

Government naturally resists reporting what they do not know.

Communities primed for panic may assume the worst case scenario.

News media will attempt to create coherence, even when there is none.

**Key Lesson #2:** (Central Dilemma) Reacting to ambiguous warning is essential but helps terrorists achieve goals.
Actual terrorist target may be damage U.S. economy.

Protective steps against uncertain threats cause widespread economic disruption.

Government action effectively implements terrorist goals.

**Key Lesson #3:** Relaxing protective measures is more difficult than imposing them.

Leaders likely will take dramatic steps to block terrorists when warning becomes more credible.

If steps are effective, we won’t see the attack.

Silence creates an ambiguous situation.

Were we successful or was it a hoax?

Did we disrupt the attack or is this a pre-set pause in the terrorist plan?

When is it safe to return to normal life?

**Key Lesson #4:** How do we avoid 20 years of economic disruption? “We have to avoid two day strategies in a twenty year war.” SAM NUNN

Relatively easy for terrorists to create credible threat.

Government leaders cannot ignore credible threat.

How do we avoid “cheap” terrorism forcing us to achieve their goals?

We need a 20 year strategy, not a one-time strategy

**Key Lesson #5:** Intelligence no longer neatly falls into “foreign” and “domestic” categories.

Modern terrorism is trans-border.

America’s intelligence operations are border-bound.

Coordination has improved, but it is still inadequate.

New Department of Homeland Security will have difficulty fixing the problem.
Key Lesson #6: The current Homeland Security Alerting System does not translate well to the Private Sector.

- Government color-coded system works for federal government.
- Not directive to State and local governments.
- Different alerting concepts in different jurisdictions.
- Preparations entirely voluntary for the Private Sector.
- No effective “report-back” system beyond federal response.

Key Lesson #7: Aviation security remains a problem.

- Enormous progress in commercial passenger aviation.
- Limited security improvement in general aviation.
- Security improvements for air cargo/air charter operations not adequate.

Key Lesson #8: Chemical Industry a key area of concern.

- Wide use of chemicals in American industry/society.
- Security procedures not necessarily designed for terrorism.
- Very complex control problem.
- Multiple producers.
- Multiple transportation methods.
- Widely distributed storage locations controlled by many different public and private organizations.

Key Lesson #9: Federal-State government interface is insufficient.

- State/local government indispensable element of response.
- Widespread misunderstanding and distrust between federal and state/local levels of government.
Current communication channels insufficient for serious crisis.

Need some “classification” system to share sensitive information but prevent public Dissemination.